Information Resource Center
American Embassy Buenos Aires
http://argentina.usembassy.gov

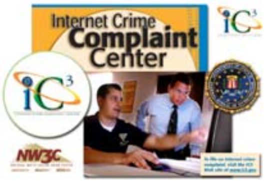
CIBERTERRORISMO

"Aunque los medios y los fines hayan evolucionado a través de la historia, los elementos esenciales del terrorismo -- miedo, pánico, violencia y dislocamiento -- han cambiado poco, hoy, un potencial destructivo tremendo cabe en paquetes fácilmente transportables (bombas, gas neurotrópico o de nervios y agentes biológicos), y las computadoras conectadas con la Internet pueden ser atacadas desde cualquier punto de la tierra". Paul Rodgers, del Centro Nacional de Protección de Infraestructuras de la Oficina Federal de Investigaciones.

Información en español

LA LUCHA CONTRA EL DELITO EN LÍNEA ELECTRÓNICA

Daniel Larkin
Periódico electrónico del Departamento de Estado de Estados Unidos, marzo de 2006



Con el comercio en línea electrónica ha hecho su aparición la delincuencia en línea. Los organismos encargados de la ejecución de la ley han ideado nuevos métodos y establecido nuevas relaciones para atrapar a los delincuentes que actúan en el espacio cibernético. Daniel Larkin es jefe del Centro de Denuncias de Delitos en Internet (IC3) en la Oficina Federal de Investigaciones (FBI).
http://usinfo.state.gov/journals/itgic/0306/ijgs/larkin.htm

CÓMO PERMANECER SEGURO EN EL ESPACIO CIBERNÉTICO

Por Lawrence R. Rogers
Periódico electrónico del Departamento de Estado de Estados Unidos,Volumen 8, número 3, noviembre de 2003

La Internet es una magnífica herramienta para la comunicación y la investigación, así como un medio de recreación para millones de personas en todo el mundo. Es también un riesgo de seguridad. Los programas de computadora creados con malas intenciones se han empleado para atacar los sistemas de computadoras conectados a la Internet mundial, con el objeto de causar daños a los programas y lograr acceso a la información confidencial. Las noticias sobre estos ataques le han dado, en todo el

mundo, un significado nuevo a palabras de vieja data como "virus", "gusano", "infección" y "caída", parte de un vocabulario alarmante que puede intimidar a quienes apenas comienzan a utilizar esta nueva tecnología. ¿Qué significa todo esto y cómo pueden los viajeros de menor experiencia en la Internet navegar por sus peligros con mayor seguridad?
http://usinfo.state.gov/journals/itgic/1103/ijgs/gj7.htm

PROTEGER A NORTEAMERICA DEL TERRORISMO CIBERNETICO

Por Paul Rodgers
Periódico electrónico del Departamento de Estado de Estados Unidos, Volumen 6, número 3, noviembre de 2001

"La necesidad de aumentar la seguridad de las operaciones críticas ha crecido marcadamente en años recientes, como resultado de la escalada del uso de la tecnología de la información para mejorar el desempeño, las presiones competitivas incrementadas resultantes de la supresión de regulaciones y la mundialización, y la concentración de operaciones en un número menor de instalaciones para así reducir costos, con la reducción resultante de redundancia y capacidad de reserva
http://usinfo.state.gov/journals/itps/1101/ijps/pj63fbi.htm

Información en inglés

THE NATIONAL STRATEGY TO SECURE CYBERSPACE

THE NATIONAL STRATEGY TO
SECURE
CYBERSPACE

The National Strategy to Secure Cyberspace is part of our overall effort to protect the Nation. It is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people.
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

CYBERCRIME: THE COUNCIL OF EUROPE CONVENTION

(CRS Report for Congress) (December 01, 2005)
Kristin Archick, Specialist in European Affairs, Foreign Affairs, Defense, and Trade Division

The Council of Europe's Convention on Cybercrime was opened for signature on November 23, 2001. The Convention is the first international treaty designed to address several categories of

crimes committed via the Internet and other computer networks. Negotiations on the Convention began in 1997, following a determination by the Council that the transnational character of cybercrime could only be tackled at the global level. Since then, the increase in hacking incidents, the spread of destructive computer viruses, and the minimal prosecution of such crimes in many states, have spurred on the Council's efforts. The September 11, 2001 terrorist attacks provided further momentum by raising the specter of cyber attacks on critical infrastructure facilities, financial institutions, or government systems, and by highlighting the way terrorists use computers and the Internet to communicate, raise money, recruit, and spread propaganda. To date, the Convention has been signed by 38 Council of Europe members and four non-members (the United States, Canada, Japan, and South Africa) that also participated in the negotiations.
http://fpc.state.gov/documents/organization/58265.pdf

FEDERAL PLAN FOR CYBER SECURITY AND INFORMATION ASSURANCE RESEARCH AND DEVELOPMENT

A Report by the Interagency Working Group on Cyber Security and Information Assurance Subcommittee on Infrastructure and Subcommittee on Networking and Information Technology Research and Development
April 2006

This report was developed by the Interagency Working Group (IWG) on Cyber Security and Information Assurance (CSIA), an organization under the NSTC. The CSIA IWG reports jointly to the Subcommittee on Infrastructure of the NSTC's Committee on National and Homeland Security, and the Subcommittee on Networking and Information Technology Research and Development (NITRD) of the NSTC's Committee on Technology. The report is published by the National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD). The NCO/NITRD supports overall planning, budget, and assessment activities for the multiagency NITRD Program under the auspices of the NSTC's NITRD Subcommittee.
http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES

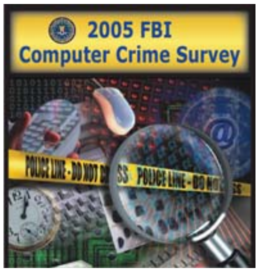
(CRS Report for Congress) (October 20, 2005)
John Rollins, Specialist in Terrorism and International Crime Foreign Affairs, Defense, and Trade Division and Clay Wilson, Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division

Cybercrime increased dramatically between 2004 and 2005, and several recent terrorist events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. This report examines possible terrorists' objectives and computer vulnerabilities that might lead to an attempted cyberattack against the critical infrastructure of the U.S. homeland, and also discusses the emerging computer and other technical skills of terrorists and extremists. Policy issues include exploring ways to improve technology for cybersecurity, or whether U.S. counterterrorism efforts should be linked more closely to international efforts to prevent cybercrime.
http://www.au.af.mil/au/awc/awcgate/crs/rl33123.pdf

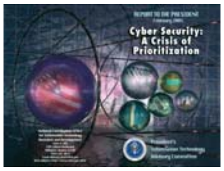
COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS (CRS Report for Congress) (Updated April 1, 2005)
Clay Wilson, Specialist in Technology and National Security, Foreign Affairs, Defense, and Trade Division

Many international terrorist groups now actively use computers and the Internet to communicate, and several may develop or acquire the necessary technical skills to direct a coordinated attack against computers in the United States. A cyberattack intended to harm the U.S. economy would likely target computers that operate the civilian critical infrastructure and government agencies. However, there is disagreement among some observers about whether a coordinated cyberattack against the U.S. critical infrastructure could be extremely harmful, or even whether computers operating the civilian critical infrastructure actually offer an effective target for furthering terrorists' goals. This report provides background information for three types of attacks against computers (cyberattack, physical attack, and electromagnetic attack), and discusses related vulnerabilities for each type of attack. The report also describes the possible effects of a coordinated cyberattack, or computer network attack (CNA), against U.S. infrastructure computers, along with possible technical capabilities of international terrorists.
http://www.au.af.mil/au/awc/awcgate/crs/rl32114.pdf

2005 FBI COMPUTER CRIME SURVEY
Federal Bureau of Investigation, January 18, 2006



This survey sought to gain an accurate understanding of what computer security incidents organizations are experiencing within the United States. It addresses a variety of issues, including computer security technologies used, security incident types, actions taken, and emerging technologies, such as wireless technology and biometrics. Responses were anonymous and encompassed a cross-section of more than 2,000 public and private organizations in Iowa, Nebraska, New York, and Texas
http://www.newleafproductions.com/ccs2005.pdf



CYBER SECURITY: A CRISIS OF PRIORITIZATION
President's Information Technology Advisory Committee, Executive Office of the President, February 2005

This report presents key findings and recommendations on how the federal government can foster new architectures and technologies to secure the nation's IT Infrastructure, such as increasing support for research in civilian cyber security.
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

COMPUTER SECURITY INCIDENT HANDLING GUIDE: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Tim Grance, Karen Kent & Brian Kim (National Institute of Standards and Technology, January 2004)

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This publication provides guidelines for handling computer security-related incidents and determining appropriate responses. The guidelines focus on detecting, analyzing, prioritizing, and handling incidents and can be followed independent of hardware platforms, operating systems, protocols, or applications
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES IN ADDRESSING CYBERSECURITY

Statement of David A. Powner, Director, Information Technology Management Issues (United States Government Accountability Office)
July 19, 2005

Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurityrelated critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve cybersecurity of our nation's critical infrastructure.
http://www.gao.gov/new.items/d05827t.pdf